Google Inc. et al v. Egger et al

Doc. 376 Att. 2

EXHIBIT 3

Dockets.Justia.com

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
tien@eff.org
KURT OPSAHL (191303)
kurt@eff.org
KEVIN S. BANKSTON (217026)
bankston@eff.org
CORYNNE MCSHERRY (221504)
corynne@eff.org
JAMES S. TYRE (083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

TRABER & VOORHEES
BERT VOORHEES (137623)
bv@tvlegal.com
THERESA M. TRABER (116305)
tmt@tvlegal.com
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103
Telephone: 626/585-9611
626/ 577-7079 (fax)

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE (121156)
wiebe@pacbell.net
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200
415/433-6382 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN, on Behalf of Themselves and All Others Similarly Situated,,

Plaintiffs,

v.

AT&T CORP., et al.,

Defendants.

No. C-06-0672-VRW

CLASS ACTION

DECLARATION OF J. SCOTT MARCUS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Date: June 8, 2006
Courtroom: 6, 17th Floor
Judge: Hon. Vaughn Walker

FILED UNDER SEAL PURSUANT TO CIVIL LOCAL RULE 79-5

TABLE OF CONTENTS

QUALIFICATIONS 2

BACKGROUND –DOCUMENTS REVIEWED 6

OVERVIEW AND SUMMARY OF PRINCIPAL OPINIONS 8

BACKGROUND – FIBER OPTICS 11

SUMMARY OF THE ARCHITECTURE OF THE SG3 CONFIGURATION AND ITS DATA CONNECTIVITY 14

CAPABILITIES OF THE SAN FRANCISCO SG3 CONFIGURATION 18

TRAFFIC CAPTURED AT SAN FRANCISCO SG3 ROOM 22

NUMBER OF LOCATIONS 27

TRAFFIC CAPTURED BY MULTIPLE SG3 ROOMS 28

ALTERNATIVE REASONS WHY AT&T MIGHT HAVE DEPLOYED THE SG3 CONFIGURATIONS 30

AT&T'S FINANCIAL CONDITION IN 2003 33

LIST OF EXHIBITS

A	Curriculum vitae of J. Scott Marcus
B	Eric Lichtblau and James Risen, Spy Agency Mined Vast Data Trove, Officials Report, The New York Times, Dec. 24, 2005
C	Barton Gellman, Dafna Linzer and Carol D. Leonnig, Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared, Washington Post, Feb. 5, 2006
D	Marcus et al, "Internet interconnection and the off-net-cost pricing principle"
E	Marcus, "Call Termination Fees: The U.S. in global perspective"
F	Marcus, "What Rules for IP-enabled NGNs?"
G	"Evolving Core Capabilities of the Internet"
H	http://en.wikipedia.org/wiki/Modulation
I	http://en.wikipedia.org/wiki/Attenuation
J	http://en.wikipedia.org/wiki/Decibel
K	ADC brochure (Value-Added Module System: LGX Compatible)
L	http://www.narus.com/solutions/IPanalysis.html
M	http://www.ist-scampi.org/events/workshop-2004/poell.pdf
N	http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf
O	http://www.narus.com/platform/index.html
P	http://www.narus.com/solutions/NarusForensics.html
Q	In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, FCC WC Docket 02-361, Petition of AT&T
R	Report of the NRIC V Interoperability Focus Group, "Service Provider Interconnection for Internet Protocol Best Effort Service"
S	Ch. 14, Marcus, Designing Wide Area Networks and Internetworks: A Practical Guide (1999)
T	http://www.broadbandweek.com/newsdirect/0208/direct020802.htm, August 2, 2002
U	http://www.narus.com/solutions/IPsecurity.html
V	http://www.fcw.com/article90916-09-26-05-Print
W	http://www.att.com/news/2004/03/22-12972

X http://www.eweek.com/print_article2/0,1217,a=139716,00.asp

Y Lehman Brothers analysis of AT&T (Jan. 24, 2003)

I, J. Scott Marcus, declare under the penalty of perjury that the following is true and correct:

1. The Electronic Frontier Foundation (EFF) has asked me to render an expert opinion[1] on the implications of a declaration by Mark Klein ("Klein Declaration"), and on a series of documents alleged to have been generated by AT&T (Exhibits A, B and C to the Klein Declaration) ("Klein Exhibits"), in conjunction with Plaintiffs' Motion for a Preliminary Injunction.

2. I am strongly of the opinion that the Klein Exhibits are authentic, and I find Mr. Klein's declaration to be fully consistent with the documents and entirely plausible.

3. The EFF specifically requested that I assess whether the program described in the Klein Declaration and Klein Exhibits is consistent with media reports about a program authorized by the President of the United States, under which the National Security Agency ("NSA") engages in warrantless surveillance of communications of people inside the United States ("the Program").

4. I was asked to review the following two news articles: Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, The New York Times, Dec. 24, 2005 (attached as Exhibit B), and Barton Gellman, Dafna Linzer and Carol D. Leonnig, *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, Washington Post, Feb. 5, 2006 at A01 (attached as Exhibit C).

5. I was asked to focus on the following claims in these two news articles, with respect to AT&T Corp.: that major U.S. telecommunications companies are assisting the government in carrying out the Program; that these companies have given the government direct access to telecommunications facilities physically located on U.S. soil; that by virtue of this access, the government can now monitor both domestic and international communications of persons in the United States; and that surveillance under the Program is conducted in several stages, with the early stages being computer-controlled collection and analysis of communications and the last stage being actual human scrutiny.

6. In the sections that follow, I present my qualifications, and provide an overview of

[1] Attached hereto as Exhibit A is my curriculum vitae.

the implications of the Klein Declaration and Klein Exhibits. I present my conclusions in regard to the scope of the program, and the volume of data that was captured. I also explain why I find credible Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale.

QUALIFICATIONS

7. For more than 30 years, I have worked in a wide range of positions involving computers, data communications, economics, and public policy. This declaration draws on my experience in several of these positions, and in several different academic disciplines.

8. From March 1990 to July 2001, I held a series of responsible positions with Bolt, Beranek and Newman (which was renamed BBN Corp.) and with its successor companies, GTE Internetworking and Genuity, culminating in my work as Chief Technology Officer (CTO) of Genuity.

9. BBN Corp. was acquired by GTE Corp. in 1997. The portion of BBN that functioned as an Internet Service Provider (ISP)[2] became GTE Internetworking, a wholly owned subsidiary of GTE.

10. In 2000, at the time of the Bell Atlantic – GTE merger (which formed Verizon), GTE Internetworking was spun out into an independent company in order to satisfy regulatory obligations relevant to the merger. The independent firm was called Genuity.

11. My primary engineering competence is as a designer of large scale IP-based[3] data networks.

12. Immediately following BBN's acquisition by GTE, I headed the team of systems architects and network engineers who developed the overall architectural design for GTE Internetworking's new data network. The team, comprising of as many as 50 senior engineers at various times, translated general business and marketing requirements into a comprehensive set of

---

[2] An *Internet Service Provider (ISP)* is an organization that enables other organizations to connect to the global Internet. ISPs often provide additional supporting services to enable electronic mail (e-mail) and to permit domain names (such as www.fcc.gov) to be recognized.

[3] All Internet traffic is *IP-based*, *i.e.* based on the Internet Protocol. I expand on this discussion in the section in which I discuss "Traffic captured".

high level engineering designs. This was a project of substantial scope and scale. The new network transformed 13,000 miles of dark fiber[4] into a single integrated network providing nationwide (and ultimately global) high speed Internet access services, and support for consumer Internet access via broadband and dial-up, and high speed data services for large enterprises. In terms both of scope and of technology, this network was at the state of the art of the day. The network was viewed as a technical and economic success, and became in short order one of the largest Internet backbone networks in the world – in terms of traffic carried, it could be viewed as the fourth largest Internet *backbone*[5] in the world for much of the time that I was there.

13. I have some experience with AT&T's network at its inception. When AT&T initially entered the Internet business in 1995, they contracted with my firm, BBN, to provide the underlying service. In effect, they "private labeled" a BBN service. They provided connections to their customers over dedicated circuits, which were cross-connected to BBN's Internet network. The customer perceived an AT&T-branded service, but BBN provided the acual ISP services. I was BBN's lead technical person for this endeavor.

14. BBN and AT&T conducted exploratory, but ultimately unsuccessful, discussions about building an Internet backbone together. AT&T ultimately decided to implement their own Internet backbone network (the Common Backbone [CBB],[6] which is the same name used in these documents), and thus to assume the ISP functions that had previously been provided by BBN. The initial design of the CBB reflected AT&T's experience in working with BBN.

15. In addition to the GTE Internetworking's own Internet backbone, and the work with AT&T, I designed a number of networks for commercial and government customers. I did the initial design work and cost analysis for a very large dial-up network for America Online in 1995.

---

4 Fiber optics are discussed later in this declaration. Dark fiber is fiber optic cable that is not yet carrying traffic.

5 The term *backbone* is widely used in the industry, but not precisely defined. An Internet backbone can be thought of as a large ISP, many of whose customers may themselves be smaller ISPs. There is no single network that is *the Internet*; rather, the Internet backbones collectively form the core of the global Internet. The term backbone is also sometimes used to denote any large IP-based network, whether used to provide IP-based services to the public or not.

6 The AT&T Common Backbone, like backbones generally, is a large IP-based network. The CBB is used for the transmission of interstate or foreign communications.

This network ultimately carried as much as 40% of America Online's dial-up traffic.

16. My experience as CTO at GTE Internetworking provides useful insights not only in network design, but also into operational procedures in a large Internet backbone operator associated with a large traditional telecommunications carrier. BBN's joint project with AT&T required me to work closely with AT&T's engineers as they deployed the service. In addition, much of BBN's Internet equipment was physically deployed into points of presence owned and operated by WorldCom and by MCI, which required that I be able to coordinate with their staffs as well. These insights into carrier operations enable me to assess the AT&T documents.

17. Many of my other duties at BBN, GTE Internetworking and Genuity are relevant to this declaration.

18. I created a network design and capacity planning function within BBN, and ran the function for several years. In the context of an ISP, capacity planning is the process whereby the ISP measures and interprets current service demands on the network, projects future demands (considering both current and projected future service offerings), and plans for necessary network enhancements to meet those demands. Capacity planning required constant interaction with the company's financial planners, as well as marketing and engineering. It also required an in-depth understanding of traffic flows within and between Internet providers. After the merger with GTE, I received a GTE Chairman's Leadership Award for that work.

19. I am the author of a textbook on data network design: *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999. The book largely reflects my experience with capacity planning and network design in the large at BBN, GTE Internetworking and Genuity.

20. I held a number of sales and marketing positions at BBN, and in those roles (and also subsequently as Genuity's CTO) frequently participated in the assessment of the costs and the potential revenues associated with new services.

21. Many of my outside consulting assignments at BBN involved elements of data security and network security. Later, as CTO, the company's senior security expert was a direct report. I thus had a general oversight role with respect to the company's performance of lawful

intercept.

22. As CTO, I also had primary responsibility for the company's strategic approach to peering[7] with other Internet Service Providers (including AT&T). I personally chaired the firm's peering policy council, where the company's various stakeholders (engineering, financial and marketing) established strategic direction in regard to peering.

23. I supported GTE's General Counsel in raising concerns about the MCI-WorldCom merger (1998) and the proposed MCI-Sprint merger (2000), arguing that the network externality effects resulting from the mergers would make anticompetitive practices as regards Internet backbone peering both feasible and profitable. These arguments hinged to a substantial degree on my ability to estimate peering traffic flows between the major Internet backbones in both real and hypothetical circumstances. This activity drew heavily on my experience with the measurement and analysis of traffic.

24. From July 2001 to July 2005, I was the Senior Advisor for Internet Technology at the Federal Communications Commission (FCC). In this role, I served as the FCC's leading technical expert on the Internet, and provided advice to the Chairman's office and to other senior managers as regards technology and policy issues.

25. I participated in numerous proceedings during my time at the FCC, including several that dealt generally with broadband and with Voice over IP (VoIP).[8]

26. I was a member of the FCC's Homeland Security Policy Council, with significant responsibilities as regards cybersecurity and infrastructure security. I held a top secret clearance. I frequently spoke on the FCC's behalf on lawful intercept (CALEA)[9] in connection with IP-based services. I was an active and significant participant in the FCC's proceedings related to CALEA in

---

[7] *Peering* is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. A more extensive definition appears later in this Declaration, under "Traffic Captured."

[8] *IP* is the Internet Protocol. All Internet data is IP-based. *Voice over IP* refers to the transmission of voice over IP-based networks – either private networks or the "public" Internet.

[9] Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279. CALEA is the statute that requires carriers to proactively instrument their networks in order to support law enforcement needs. The FCC has a role in its implementation.

connection with Voice over IP (VoIP) and with broadband.

27. From July 2005 to the present, I have been a Senior Consultant for the WIK, located in Bad Honnef, Germany. The WIK is a leading German research institute specializing in the economics of electronic communications, and the regulatory implications that flow from those economics. Much of my current work applies economic reasoning to policy problems in electronic communications.

28. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and have held several senior volunteer positions within the IEEE. I am currently co-editor for public policy and regulatory matters for *IEEE Communications Magazine*. I have also served as a trustee of the American Registry of Internet Numbers (ARIN).

29. I do not consider myself an economist, but I have a good working knowledge of economics as it applies to the aspects of telecommunications that I deal with. Several of my professional papers over the past few years are economics papers, and a number of them have been cited by recognized economists.[10] Other recent papers apply economic reasoning to problems in the regulation of electronic communications.[11]

BACKGROUND –DOCUMENTS REVIEWED

30. In forming my expert opinions in this Declaration, I reviewed the following documents: the Klein Declaration; *SIMS Splitter Cut-In and Test Procedure*, Issue 2, 01/13/03

[10] See, for instance, my paper with Jean-Jacques Laffont, Patrick Rey, and Jean Tirole, IDE-I, Toulouse, "Internet interconnection and the off-net-cost pricing principle," *RAND Journal of Economics*, Vol. 34, No. 2, Summer 2003, available at http://www.rje.org/abstracts/abstracts/2003/rje.sum03.Laffont.pdf (Exhibit D). An earlier version of the paper appeared as "Internet Peering," *American Economics Review*, Volume 91, Number 2, May 2001. See also "Call Termination Fees: The U.S. in global perspective," presented at the 4th ZEW Conference on the Economics of Information and Communication Technologies, Mannheim, Germany, July 2004, available at: ftp://ftp.zew.de/pub/zew-docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf (Exhibit E). Another paper that deals primarily with economics has been commissioned by the International Telecommunications Union (ITU-T) for presentation at their ITU New Initiatives Workshop on "What Rules for IP-enabled NGNs?," March 23-24, 2006: "Interconnection in an NGN environment," available at http://www.itu.int/osg/spu/ngn/documents/Papers/Marcus-060323-Fin-v2.1.pdf (Exhibit F).

[11] *See*, for instance, "Evolving Core Capabilities of the Internet," *Journal on Telecommunications and High Technology Law*, 2004 (Exhibit G).

(Klein Decl. Exh. A); *SIMS Splitter Cut-In and Test Procedure: OSWF Training*, Issue 2, January 24, 2003 (Klein Decl. Exh. B); and *Study Group 3 LGX/Splitter Wiring: San Francisco*, Issue 1, 12/10/02 (Klein Decl. Exh. C).

31. I have also reviewed publicly available data on the Internet – wherever I have relied on such data, I have so indicated in the text.

32. The Klein Exhibits use terms such as "SG3 equipment" and "SG3 room." I believe *SG3* to be an acronym for *Study Group 3*, which is used consistently to describe the project. Consistent with this terminology, I will refer to the *SG3 Configuration* throughout this declaration.

33. I interpret *OSWF* as a reference to the *On Site Work Force*. These documents represent directions to technicians who must "cut" the new facilities into the network, *i.e.* install them with as little impact as possible on AT&T's ongoing network operations.

34. Based on my experience in working with AT&T, I consider the documents to be written with the meticulous attention to detail that is typical of AT&T operations. Highly skilled central engineering staff provided unambiguous and highly detailed directions in order to enable implementation by multiple on site field crews at a lower skill level. Any operations that could be done in advance were dealt with prior to the cut. The cut was designed to be as fast and as painless as possible, so as to minimize the risk of network disruption. The cut was to take place during the maintenance window (presumably during the early morning hours, *e.g.* 2:00 AM) so as to further minimize possible disruption.[12]

35. It is clear that these plans relate to real deployments, and not just to a theoretical or hypothetical exercise. The last page of Klein Exhibit B makes clear that the San Francisco deployment was already in full swing when the document was published on January 24, 2003. Of sixteen large peering circuits that were to be diverted, (1) circuit engineering was complete for eight, (2) actual change orders had already been issued for four, and were scheduled to be issued for four more within the subsequent week (i.e. by 1/30/2003), and (3) request dates had been established for the completion of the remaining circuit engineering, for splitter pre-test and for

[12] *See* Klein Exh. A, page 4.

putting the splitters into the circuits, all in 1/2003 and 2/2003.

36. Klein Exhibit B and Klein Exhibit C are specific to AT&T's San Francisco facility, but Klein Exhibit A is generic – it is relevant to all sites where this cut was to take place.

OVERVIEW AND SUMMARY OF PRINCIPAL OPINIONS

37. My expert assessment is based on the Klein Declaration, the AT&T documents collectively designated as the Klein Exhibits, my extensive and varied experience in the industry, and various publicly available documents. Where I have relied on such documents, I have so indicated in the text.

38. Based on these documents, other publicly available documents, and my general knowledge of the industry, I conclude that AT&T has constructed an extensive – and expensive – collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well.*[13]

39. In terms of the media claims I was asked to evaluate with respect to AT&T, I conclude that: the infrastructure described by the Klein Declaration and Klein Exhibits provides AT&T Corp. with the capacity to assist the government in carrying out the Program; that the infrastructure deployed included a data network (the *SG3 backbone*) that apparently provided third party access to the SG3 room or rooms; that, if the government is in fact in communication with this infrastructure, AT&T Corp. has given the government direct access to telecommunications facilities physically located on U.S. soil; that, by virtue of this access, the government would have the capacity to monitor both domestic and international communications of persons in the United States; and that surveillance under the Program is conducted in several stages, with the early stages being computer-controlled collection and analysis of communications and the last stage being actual human scrutiny.

40. A key question is whether the infrastructure that AT&T deployed – which I refer to for purposes of this declaration as the *SG3 Configurations* – is being used solely for legitimate or

[13] Later in this Declaration, I provide my assessment of the volume of domestic and international traffic captured.

innocuous purposes, or for interception that violates consumer privacy and U.S. law. The SG3 Configurations could be used for a number of legitimate purposes; however, the scale of these deployments is, in my opinion and based on my experience, vastly in excess of what would be needed for any likely application, or any likely combination of applications other than surveillance.

41. The SG3 Configurations that were deployed are not routine for Internet backbone operators, and they are emphatically not required (nor, apparently, are they being used) for the transmission of Internet data between customers.

42. I consider other possible alternative hypotheses for AT&T's deployments later in this Declaration, under "Alternative reasons why AT&T might have deployed the SG3 Configurations." For instance, the SG3 Configurations could be used in support of routine lawful intercept, and are possibly being used in that way, but lawful intercept requirements could not account for AT&T's deployment of the SG3 deployments. As another example, the SG3 Configurations could be used in support of AT&T commercial security offerings, and it appears that AT&T is using either the SG3 Configurations or, more likely, similar technology deployed elsewhere in support of their Internet Protect commercial offering. In my judgment, and based on my experience, it is highly unlikely that benign applications, either individually or collectively, provided the rationale for the deployment. The information at hand suggests, rather, that AT&T has attempted after the fact to find ways to realize additional commercial value out of a very substantial deployment that had already been made primarily in order to conduct (presumably warrantless) surveillance. Public statements by AT&T officials over the years tend to support this view – AT&T only belatedly realized that customers might be interested in certain of these capabilities.[14]

43. Prior to seeing the Klein Declaration, I would have expected the Program to involve a modest and limited deployment, targeted solely at overseas traffic, and likely limited in the information captured to traffic measures (except pursuant to a warrant). The majority of international IP traffic enters the United States at a limited number of locations, many of them in the areas of northern Virginia, Silicon Valley, New York, and (for Latin America) south Florida.

[14] Supporting detail appears later in this Declaration, in "Alternative reasons why AT&T might have deployed the SG3 Configurations."

This deployment, however, is neither modest nor limited, and it apparently involves considerably more locations than would be required to catch the majority of international traffic.

44. The SG3 Configurations are fully capable of pattern analysis, pattern matching and detailed analysis at the level of *content*, not just of addressing information. One key component, the NARUS 6400, exists primarily to conduct sophisticated rule-based analysis of content. It is also well suited to high speed data reduction – to the "winnowing down" of large volumes of data, in order to identify only events of interest.

45. Klein Exhibit C speaks of a private SG3 backbone network, which appears to be partitioned from AT&T's main Internet backbone, the CBB.[15] This suggests the presence of a private network. The most plausible inference is that this was a covert network that was used to ship data of interest to one or more central locations for still more intensive analysis. I return to the capabilities of the SG3 Configurations later in this Declaration, under "Capabilities of the SG3 Configuration."

46. Given the probable cost of these configurations, and the likely limited commercial return, I find it exceedingly unlikely a financially troubled AT&T[16] would have made these investments at that time on its own initiative. I can envision no commercial reason, nor any combination of commercial reasons, that would render that investment likely. I therefore conclude that it is highly probable that funding came from an outside source, and consider the U.S. Government to be the most likely source. This supports Mr. Klein's assertion that the room was an NSA secure room, accessible only to NSA-cleared personnel.

47. I also find that the components that were chosen are exceptionally well suited to a massive, distributed surveillance activity (*see* "Capabilities of the SG3 Configuration" later in this Declaration). No other application provides as good an explanation for the combination of engineering choices that were made.

48. In addition, the private SG3 backbone network referred to in Klein Exhibit C,

---

[15] Klein Exh.C, pp 6, 12, 42. Again, *see* "Capabilities of the SG3 Configuration" later in this Declaration.

[16] I return to the topic of AT&T's financial condition later in this Declaration, under "AT&T's Financial Condition in 2003."

appears to be partitioned from AT&T's main Internet backbone, the CBB.[17] This is perfectly consistent with the notion of massive, covert distributed surveillance system. It is not consistent with normal AT&T practice – they have been working for years to try to reduce the number of networks in use, in the interest of engineering and operational economy.

49. For all of these reasons, I am persuaded that the SG3 Configurations were deployed primarily in order to perform surveillance on a massive scale, and not for any other purpose.

BACKGROUND – FIBER OPTICS

50. The Klein Declaration speaks (at ¶ 24 and in the sections following) of *splitting* the light signal, so as to divert a portion of the signal to the SG3 Secure Room. It may be helpful to review (at an informal level suitable for a non-specialist) some of the characteristics of fiber optic transmission before proceeding.

51. Historically, electronic communications were carried over copper wires, or were broadcast through the air. In both instances, it was often economically and technically advantageous to *modulate*[18] the signal onto a higher frequency wave. Doing so enables the recipient to select from among multiple signals transmitted over the same physical medium. You do this every time that you tune your television or radio to a particular channel.

52. More recently, fiber optics have supplanted the use of copper wire for many applications, especially those involving long distances. Instead of modulating signals onto electrical waves or radio waves, they are modulated onto light waves. Because light waves have a much higher frequency than the waves used in copper wires, it is possible to modulate far more information onto them.

53. Fiber optics have an additional advantage over copper wires: They do not generate electrical interference, nor are they vulnerable to it. In addition, it is difficult to "tap" into a fiber

---

[17] Klein Exh.C, pp 6, 12, 42. Again, *see* "Capabilities of the SG3 Configuration" later in this Declaration.

[18] *Modulation* is ". . . the process of varying a carrier signal, typically a [signal in the shape of a sine wave], in order to use that signal to convey information . . . . There are several reasons to modulate a signal before transmission in a medium. These include the ability of different users sharing a medium (multiple access), and making the signal properties physically compatible with the propagation medium." *See* http://en.wikipedia.org/wiki/Modulation (Exhibit H).

optic cable without detection. All of these characteristics are felt to make fiber more reliable and more secure than copper.

54. At the same time, these characteristics mean that law enforcement has to work harder to implement lawful intercept. The Hollywood image of an FBI agent with a pair of alligator clips is a thing of the past.

55. This is one of the main reasons why CALEA obligates carriers to instrument their networks in order to support requests for lawful intercept. Lawful intercept in today's world depends on the cooperation of the carrier.

56. In this case, the splitter (described below) provides an equivalent function to that of the alligator clips. However, instead of capturing traffic to a single target, these splitters collectively transferred all or substantially all of AT&T's off net IP-based traffic[19] (so-called Internet *peering*[20] traffic to other Internet backbones) to a secure room.

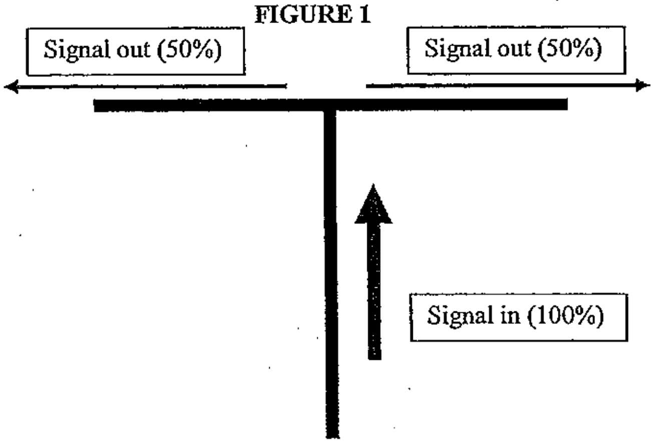
57. A splitter is a standard bit of optical gear. The simplest form is a "T" – one signal comes in, two signals go out. The splitters in this case were 50/50 splitters, which is to say that they split the signal such that 50% went to each output fiber. *See* the figure immediately below.

---

[19] The basis for this statement is developed over the balance of this Declaration. Traffic from one AT&T customer to another AT&T customer is *on net* traffic; traffic from an AT&T customer to a customer of some other ISP is in general *off net* traffic. As previously noted, all Internet traffic is *IP-based*, *i.e.* based on the Internet Protocol. I expand on this discussion in the section in which I discuss "Traffic captured."

[20] Again, peering is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers.

FIGURE 1



58. To the layman, it may seem strange that one can split a signal and still use both portions. In everyday life, if we divide something in half, each half is in some sense less than the whole. It is important to remember that, in this case, what is important is the bits (the information carried), not the underlying medium. This is more akin to making a copy of an audio CD – the CD that has been copied is not harmed by being copied. The copy contains the same information as the original.

59. Opto-electronic equipment is routinely designed to recover as much information as possible from weakened signals in order to attempt to compensate for *attenuation*[21] (weakening, or loss of "punch") of the signals over distance.

60. The AT&T designers were well aware that splitting the signal would make it weaker. They expected a loss of 4 dB[22] as a direct result of splitting the signal in two, and a loss of an additional 2 dB due to possible inefficiencies in the process – think of this latter loss as being the equivalent of friction in a mechanical device. This makes for a combined loss of 6 dB. As long

[21] "In telecommunication, *attenuation* is the decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path to the detector, but not including the reduction due to geometric spreading." *See* http://en.wikipedia.org/wiki/Attenuation (Exhibit I).

[22] dB is the standard abbreviation for decibel. "The decibel (dB) is a measure of the ratio between two quantities, and is used in a wide variety of measurements in acoustics, physics and electronics. . . . It is a "dimensionless unit" like percent. Decibels are useful because they allow even very large or small ratios to be represented with a conveniently small number. This is achieved by using a logarithm." *See* http://en.wikipedia.org/wiki/Decibel (Exhibit J).

as the loss was less than 7 dB, they presumably expected it to be within the normal operating tolerances of the devices on both ends, so they apparently made no provision to correct for the loss. They required technicians to carefully record signal levels before and after the cut (the insertion of the splitters into the operating network), and to report any loss of signal great enough to cause problems to the Network Operations Center (NOC) in Bridgeton, New Jersey.[23]

61. For the work that was described in the Klein Exhibits, each high speed circuit was apparently comprised of multiple fiber optic cables. AT&T chose to connect the cables associated with certain circuits to the splitters, and thereby to divert or copy the signals carried on those circuits. They presumably chose not to connect the cables associated with other circuits to the splitters, and thereby to refrain from diverting or copying the signals associated with those circuits.

62. In the context of the SG3 Configurations, the new splitters and a collection of optical cross-connect cables directed 50% of the signal to complete the same path that the signal had previously taken (from the CBB router to the optical transmission equipment), and directed the other 50% of the signal to the SG3 Equipment.[24] This arrangement enabled the circuits to continue to function just as they previously had, but also made the signals available to the SG3 Equipment.

63. The splitter configuration that AT&T used is routinely available from a major supplier of equipment for electronic communications, ADC. *See* line 1 of page 4 of ADC's brochure "Value-Added Module System: LGX[25] Compatible," available at http://www.adc.com/Library/Literature/891_LGX.pdf (Exhibit K).

SUMMARY OF THE ARCHITECTURE OF THE SG3 CONFIGURATION AND ITS DATA CONNECTIVITY

64. In this section, I provide a summary overview of the architecture of the SG3 Configuration and its data connectivity, based on the Klein Declaration, the Klein Exhibits, and my professional expertise. More details are provided in later sections of this declaration.

---

23 *See* Klein Exh. A, p. 10.

24 See, for instance, Figure 5 on page 11 of Klein Exhibit A. Note, too, that the tables on pages 6 and 7 of Klein Exhibit C refers to "50/50 Dual Splitters."

25 The LGX refers to the format of the physical rack into which the equipment is designed to be deployed. Lucent developed the LGX format. LGX stands for Light Guide Crossconnect.

65. The Klein Declaration refers to a "secret" room being constructed within AT&T Corp.'s Folsom Street Facility, called the "SG3 Secure Room." Klein Decl., ¶ 12.

66. While Mr. Klein worked at the Folsom Street Facility, where he oversaw its WorldNet Internet room,[26] his duties included the installation of new fiber-optic circuits with respect to AT&T's WorldNet Internet service.[27] Klein Decl., ¶¶ 15, 20.

67. In the course of his employment by AT&T, Mr. Klein reviewed the three documents collectively referred to as the Klein Exhibits. Klein Decl., ¶¶ 25-26, 28.

68. The SG3 Configuration, for purposes of my declaration and expert opinions, includes the following basic elements: a room referred to in the Klein Declaration as the "SG3 Secure Room," *id.*, ¶ 12 and Klein Exh. C, p. 46, "SG3 Room," *id.*, p. 45, "SG3 Room LGX," *id.*, p. 13, "SG3 Equipment Room," *id.*, p. 41, and "SG3 Equipment," *see* Klein Decl., Exh. A, p. 10, Fig. 4; sophisticated computers and other electronic devices located in or to be installed in this room; sophisticated routers and switches capable of switching traffic among the computing systems in the room, and also to other locations; and cables associated with data circuits entering and exiting this room.

69. The SG3 Secure Room that Mr. Klein describes in his declaration is fully consistent with the various SG3 rooms referred to in the Klein Exhibits.

70. The Klein Exhibits describe procedures for splitting or diverting peering communications traffic associated with AT&T Corp.'s Common Backbone (CBB) fiber-optic network by means of splitters[28] that fed into the SG3 Secure Room.

71. By following these procedures, all the communications carried on the associated fiber optic circuits were diverted or copied to the SG3 Secure Room and could be made available

[26] The WorldNet Internet room and its equipment as described by Mr. Klein is a facility for transmitting both domestic and international wire or electronic communications by electromagnetic, photoelectronic or photooptical means. Klein Decl., ¶¶ 15, 19, 22.

[27] The AT&T WorldNet Internet service provides its users with the ability to send or receive email, to browse the web, and to send or receive other wire or electronic communications.

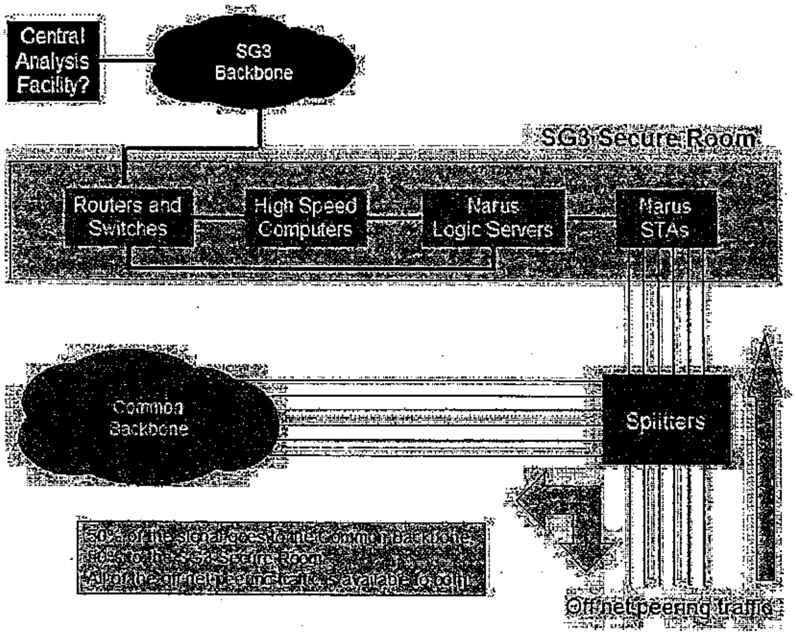
[28] I explained the function of a *splitter* earlier in this declaration, in the section on "Background – Fiber Optics". The T splitters used by AT&T apparently sent 50% of the input signal to each of two optic fiber cables, one of which conveyed the traffic to the SG3 Secure Room.

to any devices in that room.

72. With respect to the SG3 Secure Room in San Francisco, the process resulted in the diversion of all, or substantially all, of AT&T's peering traffic at the Folsom Street San Francisco facility to SG3 equipment, with no significant adverse impact on AT&T's continuously operating CBB Internet backbone.

73. The figure below helps to clarify these relationships. Splitters take the peering traffic from other networks ("off net" traffic) and route 50% of the signal to the CBB, and 50% of the signal to the SG3 Secure Room. Even though only 50% of the *signal* goes to each side of the split, all of the associated *traffic* is available both to the CBB and to the equipment in the SG3 Secure Room.

FIGURE 2



Central Analysis Facility?
SG3 Backbone
SG3 Secure Room
Routers and Switches
High Speed Computers
Narus Logic Servers
Narus STAs
Common Backbone
Splitters
Off net peering traffic

74. The Klein Exhibits also list equipment linked to or contained in the SG3 Secure Room. These include sophisticated computers and other electronic equipment. See Klein Exh. C, p. 3 ("cabinet naming"). At the same time, the Klein Exhibits do not indicate the quantities of

equipment, nor do they indicate the precise interconnections between them; consequently, the connections depicted within the SG3 Secure Room in Figure 2 should be considered to be suggestive but not necessarily exact.

75. An important group of devices in the SG3 Secure Room is the Narus STA 6400, which is a "semantic traffic analyzer," and the Narus Logic Server.[29] As I explain in more detail below, the Narus system is designed to apply logical tests to large volumes of data in real time. It is well suited to the initial screening function of a comprehensive surveillance system – in fact, surveillance is one of the system's primary functions.[30]

76. The Klein Exhibits also refer to the "SG3 backbone" and to the "SG3 backbone circuit[s]."[31] Klein Exh. C, pp. 6, 12, 42. As I explain in more detail below, it is highly likely that this SG3 backbone provides a fiber-optic network connected to the SG3 Secure Room, but separate and distinct from the CBB. In other words, while the SG3 Secure Room is connected to the CBB (from which it receives communications), it is also connected to another network, and signals can be sent out of or into the SG3 Secure Room over the SG3 backbone.

77. In sum, the general architecture of the SG3 Configuration is that communications on the CBB are split by means of splitters in a splitter cabinet, and that these communications feed into the SG3 Secure Room where they can be processed by the equipment in the SG3 Secure Room. At the same time, the SG3 backbone provides a separate, two-way channel of communication with the SG3 Secure Room. The documents reviewed do not, however, indicate what entities can receive signals or information from or send signals or information into the SG3 Secure Room via the SG3 backbone. I consider it highly probable that one or more Centralized Processing Facilities exist, as shown in Figure 2, but that belief is based on the nature of the job that the Narus system is designed to do, rather than being based on the Klein Exhibits themselves.

---

[29] See Klein Exh. C, p. 3 ("cabinet naming"). The Narus Logic Server is apparently implemented in conjunction with a Sun V880 computing system, possibly as software running on the Sun V880.
[30] See http://www.narus.com/solutions/IPanalysis.html (Exhibit L).
[31] In the text, both the SG3 backbone circuits and the peering circuits are referred to in the singular. I believe that these are grammar errors on the part of the author, and that both should have appeared in the plural.

CAPABILITIES OF THE SAN FRANCISCO SG3 CONFIGURATION

78. In this section, I explain my expert opinions about the activities likely to be occurring in the SG3 Secure Room in San Francisco.

79. In order to understand the capabilities of this configuration, it is particularly important to understand the capabilities of the Narus *Semantic Traffic Analyzer (STA)* and the Narus Logic Server. Narus's website provides singularly little information about their offerings, but a few public sources provide useful supporting detail, notably including a presentation that Narus made to the European SCAMPI project in May, 2004, and a Narus presentation available on the website of Narus's reseller IBM.[32]

80. These devices are designed to capture data directly from a network, apply a structured series of tests against the data, and respond appropriately. According to the Narus website, "One distinctive capability that Narus is known for is its ability to capture and collect data at true carrier speeds. Every second, every minute and everyday, Narus collects data from the largest networks around the world. To complement this capability, Narus provides analytics and reporting products that have been deployed by its customers worldwide. They involve powerful parsing algorithms, data aggregation and filtering for delivery to various upstream and downstream operating and support systems. They also involve correlation and association of events collected from numerous sources, received in multiple formats, over many protocols, and through different periods of time."[33]

81. Given the very high data rates that are supported, it is likely that many sophisticated techniques are used to accelerate the processing.

82. The Narus presentation on IBM's web site[34] makes it clear that the Narus system has the ability to inspect user application data (i.e. content), and not merely protocol headers. In this context, it is worth noting that references to layer numbers reflect the OSI Reference Model,

---

[32] *See* http://www.ist-scampi.org/events/workshop-2004/poell.pdf (Exhibit M), and http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf (Exhibit N).

[33] See http://www.narus.com/solutions/IPanalysis.html (Exhibit L).

[34] See http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf (Exhibit N).

where levels 5 through 7 correspond to the application[35]:

> The Narus solution is multi-tiered. Within the platform are the first two tiers; the third tier is the application that the platform is enabling. The two Narus tiers or layers are:
>
> • Collection
> • Processing
>
> **Collection**
> The collection layer in the Narus solution consists of High Speed Analyzers which connect to the network at the points where the traffic to be monitored can be most efficiently accessed. The Narus HSA's are passive and as such have zero impact on the service delivery. The HSA's analyse each and every IP packet looking at the OSI layer 2 to layer 7 data and extract layer 4 flows and ***layer 7 application data*** [emphasis added] for every IP session. Appropriate layer 4 and layer 7 data is packaged up and passed to the downstream processing layer as Narus vectors.
>
> **Processing**
> The processing layer in a Narus deployment is the LogicServer. The LogicServer process runs RuleSets which are programs that apply the business logic to the Narus vectors passed by the collection layer.

83. The statements in the IBM document make clear that the Narus system is well suited to process huge volumes of data, including user content, in real time. It is thus well suited to the capture and analysis of large volumes of data for purposes of surveillance.

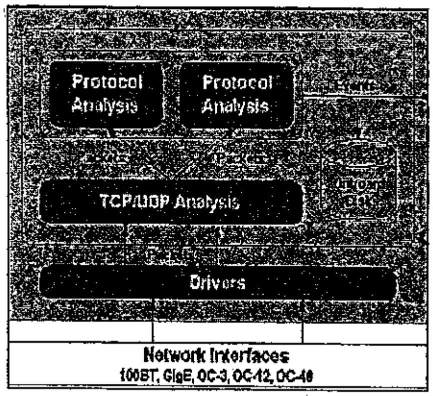
84. The following figure, which is taken from the Narus presentation to SCAMPI, makes it clear that the system, in addition to its other capabilities, is designed to identify traffic of interest and to act on it. It has the ability to store interesting traffic to the onboard disk that is part of the system.

---

[35] The Narus website is consistent with this assessment. "Stateful, Real-Time analysis of all of the traffic, Layer 3 to Layer 7 stack". The reference is to the largely obsolete OSI Reference Model of Interconnection, where levels 5 through 7 correspond to the application. See http://www.narus.com/platform/index.html (Exhibit O). For a non-technical explanation of protocol layering in the context of the Internet, *see* section 2 of my paper "Evolving Core Capabilities of the Internet," *Journal on Telecommunications and High Technology Law*, 2004 (Exhibit G).

FIGURE 3

Semantic Traffic Analyzer



85. In addition to its real time capabilities, the Narus offering can subsequently analyze large volumes of data in order to reconstruct session content as needed from the captured collections of packets. This would include e-mail, web browsing, voice over IP (VoIP), and other common kinds of Internet communication.[36]

86. It would, in my judgment, be an error to evaluate the capabilities of this configuration – substantial though they are – solely on the basis of the equipment deployed by AT&T to the SG3 Room. The AT&T documents clearly indicate the presence of an SG3 *backbone* network, apparently operating at OC-3 speeds (155 Mbps).[37] This network, while much smaller than AT&T's CBB Internet backbone network, is nonetheless quite substantial.

87. The SG3 backbone was logically distinct from the AT&T Common Backbone (CBB), but this does not necessarily mean that it had dedicated physical transmission facilities. It most probably operated over AT&T's standard optical fiber-based transmission systems, but using different high speed services – in effect, different circuits – than the CBB. If this network were carrying nothing more than a subset of AT&T's normal commercial traffic, they might not have

[36] Narus forensics, for example, "[r]econstructs and renders IP data captured with NarusDA (Directed Analysis), NarusLI (Lawful Intercept) or obtained from other data sources: Visually rebuilds or renders web pages and sessions; Presents e-mail with the header, body and attachments; Plays back streaming video or a VoIP call web session or other interactive medium." *See* http://www.narus.com/solutions/NarusForensics.html (Exhibit P).

[37] Klein Exh. C, pp. 6, 12, 42.

felt the need to do more – it has long been considered permissible to transmit *Sensitive but Unclassified Information (SUCI)* over separate fiber-based transmission paths. Had there been greater sensitivity about the data, it might have been protected in other ways, for instance by means of link encryption.

88. The obvious and natural design for a massive surveillance system for IP-based data, and the one most cost-effective to implement, would in my judgment be comprised of the following elements: (1) massive data capture at the locations where the data can be tapped, (2) high speed screening and reduction[38] of the captured data at the point of capture in order to identify data of interest, (3) shipment of the data of interest to one or two central collection points for more detailed analysis, and (4) intensive analysis and cross correlation of the data of interest by very powerful processing engines at the central location or locations. The AT&T documents demonstrate that equipment that is well suited for the first three of these tasks was deployed to San Francisco and, with high probability, to other locations. I infer that the fourth element also exists at one or more locations.

89. Staff to analyze the data would probably be based at the central locations. There would be no need to station analysts (as distinct from field support personnel) in the SG3 rooms where the data was collected. It is likely that the data were directly available for analysis by staff of the agency that funded the SG3 deployment (which runs counter to normal practice in the case of CALEA); otherwise, there would have been no need for a private SG3 backbone, separate from the CBB.

90. The SG3 technology could potentially be used in a number of different ways, some of which could be welfare-enhancing. The concern that must be raised in this case is that, in conjunction with the diversion of large volumes of traffic described in the Klein Declaration and the Klein Exhibits, this configuration appears to have the capability to enable surveillance and analysis of Internet content on a massive scale, including both overseas and purely domestic traffic.

38 The Narus STA appears to be ideally suited to this role. It is, as previously noted, designed to apply a large collection of tests against a huge volume of data at very high speed.

TRAFFIC CAPTURED AT SAN FRANCISCO SG3 ROOM

91. In this section, I explain my conclusions about the volume and type of communications traffic gathered by the SG3 Room in San Francisco.

92. The Klein Declaration and Klein Exhibits B & C describe traffic diversions associated with fiber-based circuits in the Folsom Street San Francisco facility.

93. All of the diverted data pertains to AT&T's Common Backbone (CBB), the IP-based network that supports AT&T's Internet access customers, and that also carries AT&T's VoIP services (voice over the Internet).[39] Nothing in the documents suggests that conventional telephony traffic was diverted to the SG3 Configuration.

94. The last page of Klein Exhibit B provides a list of CBB *peering* (defined below) links that were to be split and diverted to the San Francisco SG3 Configuration.

95. Nothing in the documents suggests that AT&T's *on net* traffic – traffic from one AT&T customer to another – was diverted at the time. AT&T may at some point in time have made some provision for its international customers (whose traffic to other AT&T customers would also be on net), but the documents provide no guidance. My assumption is that on net traffic was not diverted during the time frame to which the documents pertain.

96. Before proceeding, it is helpful to introduce and clarify some terms. *Peering* is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. The Network Reliability and Interoperability Council (NRIC), an advisory panel to the FCC, defined peering in this way:[40]

> *Peering* is an agreement between ISPs to carry traffic for each other and for their respective customers. Peering does not include the obligation to carry traffic to third

---

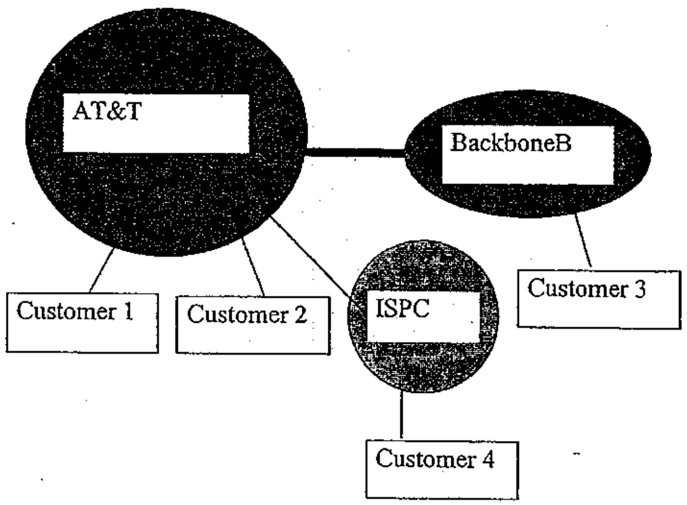
[39] See *In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges,* FCC WC Docket 02-361, Petition of AT&T, at 24 (filed Oct. 18, 2002), at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513386921 (Exhibit Q).

[40] Report of the NRIC V Interoperability Focus Group, an advisory panel to the FCC: "Service Provider Interconnection for Internet Protocol Best Effort Service," page 7, available at http://www.nric.org/fg/fg4/ISP_Interconnection.doc (Exhibit R). *See also* chapter 14 of Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999 (Exhibit S).

> parties. Peering is usually a bilateral business and technical arrangement, where two providers agree to accept traffic from one another, and from one another's customers (and thus from their customers' customers) . . . .

97. In the figure below, AT&T and Backbone B are *peers*. They have agreed to exchange traffic for their respective customers. Traffic from AT&T customer 1 to AT&T customer 2 is *on net* traffic – it remains on AT&T's network. Traffic from AT&T customer 1 to customer 3 (a customer of backbone B) is *off net* traffic.

FIGURE 4



98. In the figure, ISP C is a *transit customer* of AT&T. ISP C pays AT&T to carry its traffic, not only to AT&T customers, but to customers of other ISPs as well (such as, for example, Customer 3). In the context of this discussion, AT&T can regard traffic from Customer 4 to Customers 1 and 2 as being on net, in the sense that it does not traverse a peering connection.

99. It is perhaps also worth noting that AT&T and its peers and their many transit customers do not merely connect to the Internet; rather they *are* the Internet. The Internet is not a single, huge and over-arching network, but rather a collection of independent networks that collectively comprise a worldwide communications stratum.

100. Again, the last page of Exhibit B provides a list of CBB peering links that were to be split and diverted to the San Francisco SG3 Configuration. The sizes of these circuits are listed, with some at OC-3 (155 Mbps), some at OC-12 (620 Mbps), and some at OC-48 (2.5 Gbps). These

are all quite substantial circuits – the OC-48's are apparently on a par with the largest circuits that were in widespread use in AT&T's CBB Internet backbone at the time.

101. Traffic to and from several very large Internet providers at that time (UUNET, Sprint, Level 3 and Cable and Wireless) was delivered over OC-48 circuits. Traffic to and from another group of large providers (Verio, XO, Genuity, Qwest, Allegiance, Abovenet, and Global Crossing) was delivered over OC-12 circuits. Traffic to and from smaller, but still quite substantial, providers (ConXion, Telia and PSINet) was delivered over OC-3 circuits.

102. Large Internet backbone providers typically use direct interconnects (private peering) to exchange traffic with their largest "trading partners in bits," the firms with which they exchange the largest volume of traffic. For providers where the volume of traffic exchange at some location is large enough to warrant peering arrangements, but not large enough to justify the cost of a separate circuit for private peering, it is customary instead to interconnect with multiple peers at a so-called "public peering point" in order to exchange traffic with multiple providers there.[41] AT&T was connected to two public peering points in the San Francisco Bay area: MAE-West and the PAIX. The traffic associated with the OC-3 and OC-12 circuits to these two facilities, respectively, was also diverted to the SG3 configuration.

103. At the point where I left Genuity in July 2001 (some eighteen months before these splitters were deployed), I was intimately familiar with our traffic exchange patterns with other providers. Our measurement instrumentation ranked with the very best in the industry at that time. It is possible to draw many inferences about traffic flows among other providers from one's own traffic exchanges.

104. Based on my experience at Genuity, I believe that the traffic that was diverted represented all, or substantially all, of AT&T's peering traffic in the San Francisco Bay Area.

105. I base my reasoning on the knowledge of Genuity's peering traffic patterns, and on my general understanding of peering traffic patterns in the industry. As of July 2001, our three largest peers were WorldCom, AT&T and Sprint, collectively representing 50-60% of our traffic.

[41] *See* Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999, pages 280-282 (Exhibit S).

Our next largest peering partners changed somewhat over time, but typically included Qwest, Level3, Verio and Cable and Wireless. Public peering points such as MAE-West represented a small and steadily diminishing percentage of our peering traffic. AT&T had a larger customer base than Genuity, but one might expect the relative proportions to be generally similar, with the obvious exception of AT&T's traffic to itself. The relative sizes of peering circuits on the last page of Klein Exhibit B is not inconsistent with this assumption. Genuity had peering arrangements with 50 to 60 networks, but many of them exchanged relatively little traffic with us. All of our significant peering partners at that time appear on the list on the last page of Klein Exhibit B.

106. I therefore infer either that: (1) all of the networks with which AT&T peered in San Francisco had their traffic intercepted, or else (2) any AT&T peering partners whose traffic was not intercepted most likely were small networks that exchanged very little traffic with AT&T.

107. The traffic intercepted at the Folsom Street facility probably represented a substantial fraction of AT&T's total national peering traffic, but the percentage is unimportant for this analysis.

108. In my judgment, significant traffic to and from the plaintiffs (especially those in the San Francisco Bay Area) would have been available for interception by the SG3 Configuration, even if SG3 had only been implemented in San Francisco. As of the end of 2002, AT&T most likely had West Coast peering to other major backbones at three major locations at most: the San Francisco Bay Area, Los Angeles, and Seattle. As noted above, the major peers were present at Folsom Street, probably representing all or substantially all of AT&T's peering traffic in the San Francisco Bay Area. Off net traffic *from* the plaintiffs would have been handed off to peers at the first available opportunity (a process referred to as "shortest exit" or "hot potato" routing), and thus would with high probability have been handed off through the Folsom Street facility. Off net traffic *to* the plaintiffs could have been presented to AT&T using peering connections at any of perhaps eight different cities, so a significant fraction of the total would have passed through Folsom Street, but not all.

109. I conclude that the designers of the SG3 Configuration made no attempt, in terms of the location or position of the fiber split, to exclude data sources comprised primarily of domestic

data. A fiber splitter, in its nature, is not a selective device – all the traffic on the split circuit was diverted or copied. In my experience, backbone ISPs typically provide a single peering circuit for peering traffic at a given location – they do not provide separate circuits for domestic peering traffic as distinct from international peering traffic. Most of the backbone ISPs that appear in Klein Exhibit B had substantial U.S.-based business, and probably carried significantly more domestic traffic than international.

110. Once the data has been diverted, there is nothing in the data that reliably and unambiguously distinguishes whether the source or destination is domestic or foreign. AT&T would know with near certainty the location of the side of the communication that originated or terminated with its own customer (nearly always domestic in this case), but it would be limited in its ability to determine the location of the other side of the communication. This is because *IP addresses, unlike phone numbers, are not associated with a user's physical location.*

111. There are software programs that attempt to infer physical location from an IP address (a process referred to as *geolocation*). Geolocation is an inherently error-prone process, but some vendors claim, rightly or wrongly, an accuracy of 95% or better. The question of correctness must, however, be considered in the context of the accuracy required. When the FCC considered the geolocation problem in terms of its impact on VoIP users seeking access to emergency services, we were concerned with the possibility of identifying the user's location with sufficient accuracy to enable a policeman or ambulance driver to physically find the caller. In this case, however, it is only necessary to determine whether an IP address is inside the United States. Assuming *arguendo* that the data intercepted by the SG3 Configurations was indeed captured for purposes of surveillance, it is possible that purely domestic communications could have been excluded with a reasonably high success rate. It is nonetheless safe to say that, even had there been a serious attempt to exclude purely domestic communications, some purely domestic communications would have slipped through the filter and been analyzed anyway.

112. The documents provide no basis on which to determine whether geolocation was attempted. Given (under the foregoing assumptions) that all of the international data was going to be evaluated by a sophisticated high speed inference engine (the Narus system) in any case, the

simpler, cheaper and more natural engineering approach would be to use the Narus system to evaluate all of the data, both domestic and foreign, and to leave it to the inference engine to determine which data was interesting.

NUMBER OF LOCATIONS

113. The Klein Declaration states that splitter cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego. Unlike most statements in the Klein Declaration, this one is not based on his first hand knowledge. It is therefore appropriate to consider first, whether the assertion is plausible, and second, how large a total deployment it implies.

114. Based on my assessment of the AT&T documents, I consider the assertion to be plausible, and to be consistent with an overall national AT&T deployment to from 15 to 20 sites, possibly more.

115. Klein Exhibit B talks about general AT&T naming conventions, and says: "Since this document is designed to cover all sites, this uniform naming convention will be used. Site-specific engineering will use the LGX FIC[42] code rather than the naming."[43] This emphasis on a standardized, cookie-cutter approach is consistent with AT&T standard practice, but also implies a planned deployment to multiple sites, surely more than two or three.

116. All of these documents need to be understood in terms of AT&T practices and priorities. AT&T is used to operating networks on a large scale, with centralized highly skilled engineers and with a field force at a lower skill level. This implies the need for a highly structured approach to describing the work to be done, and precise, meticulous instructions. AT&T had clearly gone to great lengths to standardize the design of their CBB locations as much as possible; nonetheless, for a variety of reasons, the locations were not identical. The directions therefore try to strike a balance between first describing the general case for all locations, and then providing site-specific directions that apply the general directions to the circumstances of a particular CBB

---

42 As previously note, the LGX refers to an equipment rack. I infer that the FIC code refers to an AT&T convention that assigns a unique and unambiguous identifier that is suitable for site-specific work.

43 Klein Exh. B, p. 4.

location.

117. Page 5 of Klein Exhibit A discusses the various racks (LGXes) involved, and says of the Network Facing LGX: "In a majority of cases (possibly all) this will be LLGX4." (Note that the racks associated with AT&T's Common Backbone [CBB] are assigned sequential identifiers from LLGX1 to LLGX14.) If the planned deployment were for only two or three sites, the universality of LLGX4 would not have been in doubt. This again hints at a large enough deployment that it was inconvenient to check all of the necessary background plans.

118. On the same page, Klein Exhibit A refers to four different rack arrangements that could be present at any given site. On site staff would only need to familiarize themselves with the single configuration present at their site. This implies an absolute minimum of four sites; however, I consider it unlikely that they would go to this much trouble in crafting such general language if that were the case. Klein Exhibit A specifically states on page 17: "The only site with LGX Arrangement 4 is Atlanta." The absence of similar statements for Arrangements 1, 2 and 3 implies that there are two or more instances of each of those rack arrangements. Again, this is consistent with a deployment to 15 to 20 SG3 Room sites if not more.

TRAFFIC CAPTURED BY MULTIPLE SG3 ROOMS

119. I have already explained that an enormous amount of Internet traffic is likely to have been captured by the devices in the SG3 Room in San Francisco. I now briefly consider the volume of Internet traffic that would be captured if there were multiple SG3 rooms.

120. Assuming that AT&T deployed SG3 Configurations to as many locations as appears to have been the case, it is highly probable that all or substantially all of AT&T's traffic to and from other Internet providers anywhere in the United States was diverted.

121. If Internet backbone A were carrying x% of all Internet traffic, and if its customers were no more likely to interact with other A customers than with any other provider's customers, then one would expect x% of backbone A's traffic would stay on net and that 100% - x% of A's traffic would go off net (to other providers).[44] In practice, a somewhat higher fraction usually stays

[44] This is the same methodology used in my paper with Laffont, Tirole and Rey. Exhibit D, pp. 373-74.

on net for a variety of reasons.

122. Based on my knowledge of Genuity's traffic flows in 2001, and based also on AT&T's claims that it had grown to become the largest Internet backbone as of late 2002,[45] I would estimate that AT&T was carrying something like 20% of U.S. Internet backbone traffic in late 2002. This estimate reflects the assumption that Genuity's traffic pattern was fairly typical of that of other providers. If AT&T was carrying 20% of all U.S. Internet traffic, and if AT&T customers were no more likely to communicate with other AT&T customers than with customers of any other ISP, then one would expect that about 100% - 20% = 80% of AT&T customer traffic would be destined off net. Given that some traffic tends to stay on net for other reasons – for example, traffic between multiple sites of the same corporation, all of which use AT&T as a provider – I would estimate that somewhere between 60% and 80% of AT&T's customer traffic was going off net.

123. This implies that nearly all of AT&T's international traffic was diverted, with the apparent exception of traffic from an AT&T customer to an overseas AT&T customer.[46]

124. *It also implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted, representing all or substantially all of the AT&T traffic handed off to other providers.* This proportion is somewhat less than the 60%–80% estimated above, because it excludes the international traffic.

125. The volume of *purely domestic* communications available for inspection by the SG3 Configurations thus appears to be very substantial. *I estimate that a fully deployed set of SG3 Configurations would have captured something in the neighborhood of 10% of all purely domestic Internet communications in the United States.* This estimate follows from my previous estimates. The SG3 Configurations intercepted more than 50% of all AT&T domestic traffic, which

---

[45] See remarks of Hossein Eslambolchi, AT&T labs president and chief technology officer, quoted in BroadbandWeek Direct at http://www.broadbandweek.com/newsdirect/0208/direct020802.htm, August 2, 2002 ("AT&T has been steadily growing its backbone traffic and now expects to surpass WorldCom as the sector leader in a few months ...") (Exhibit T).

[46] To the extent that AT&T has overseas customers, their traffic to other AT&T customers would not appear as peering traffic and therefore would not be intercepted by the SG3 Configurations as described in the AT&T documents.

represented perhaps 20% of all Internet traffic in the United States: 20% * 50% = 10%.

126. It must be emphasized that this estimate does not mean that traffic was intercepted merely for 10% of AT&T customers; rather, it means more than half of all Internet traffic was likely intercepted (at least, at a physical level) for *all* AT&T customers. Moreover, it means that about 10% of all U.S. Internet traffic was physically intercepted for *all* U.S. Internet users, including non-AT&T customers.

127. The estimate of 10% also assumes that only AT&T implemented SG3 Configurations or their equivalent, since the AT&T deployments are the only ones that are demonstrated by the documents that I was asked to review. If other carriers had deployed configurations similar to the SG3 Configurations – feeding in, for example, to the same centralized correlation and analysis center or centers – then the percentage would of course be higher.

ALTERNATIVE REASONS WHY AT&T MIGHT HAVE DEPLOYED THE SG3 CONFIGURATIONS

128. The Klein Declaration states that the SG3 area was a Secure Room, and that only NSA-cleared personnel were permitted to enter. In this section, I consider whether it is credible that the SG3 Room described in the AT&T documents was in fact a secure facility funded by the government. I conclude that it is highly probable.

129. Given the size and the scope of the build-out, and given AT&T's financial difficulties at the time, I consider it highly unlikely that AT&T undertook the development on its own. There is no apparent commercial justification.

130. First, the SG3 Configuration is not useful for carrying Internet traffic. No provider wants to make duplicate copies of the same packets – it costs money to transport the packets, and they provide no corresponding benefits to the user.

131. Second, AT&T might have deployed the SG3 configurations in order to sell security services to their customers. AT&T does in fact offer a service called Internet Protect to its Internet access customers, and the service appears to be based on the Narus offering. Indeed, this is the

rationale indicated on the Narus website.[47] Indications are that the service has not been nearly profitable enough to justify the SG3 expenditure;[48] still it is possible that AT&T might have overestimated demand.

132. This explanation also falls short. The SG3 Configurations were deployed beginning in early 2003, meaning that planning was probably under way six to twelve months earlier, given AT&T process. Internet Protect was not announced until March, 2004.[49] Aside from that, AT&T officials themselves characterized aspects of Internet Protect as something that they had already deployed for other purposes, and only belatedly realized might benefit their customers.[50] All indications are the Internet Protect was an attempt to extract commercial value from a deployment already made – or more likely, from a new deployment using the same technology as the SG3 Configuration – rather than having been the original rationale for the deployment.

133. Third, it is possible that AT&T might have deployed the SG3 configuration in order to meet obligations for lawful intercept. The Narus system can be used for this purpose; however, it is not credible that this was the rationale for the deployment. Far simpler and far less expensive solutions could have met all the limited CALEA requirements that were in force at the time of

---

[47] "AT&T uses NarusSecure to monitor traffic in their backbone, analyzing over 2.6 petabytes of data a day. AT&T is able to provide early warnings to their security center operators, who are able to alert and inoculate their enterprise customers." See http://www.narus.com/solutions/IPsecurity.html (Exhibit U).

[48] "AT&T has packaged that help in a service it calls AT&T Internet Protect, but so far few large agencies have signed up. Buying managed security services from AT&T and other carriers might take some time to catch on, if it ever does, said Timothy McKnight, chief information security officer at Northrop Grumman. "There's a lot of value there, and I agree they should bring it to the table," he said." *See* http://www.fcw.com/article90916-09-26-05-Print (Exhibit V).

[49] http://www.att.com/news/2004/03/22-12972 (Exhibit W).

[50] "Project Gemini, for which development began nearly a year ago, sprang from AT&T's belief that it could better manage customers' security by having the defenses on the company's IP backbone network rather than simply administering security devices on the customers' premises. . . . In addition to the network-based services, AT&T is also working on a security event management system called Aurora that it plans to sell as a software solution. The system relies on the company's Daytona database and is designed to do more than simple event correlation and normalization. . . . AT&T has been using Aurora internally for approximately 18 months, Amoroso said, and only started selling the event management system on a limited basis recently after a customer saw the system and asked for it." Eweek, "Security on the Wire", November 22, 2004, at http://www.eweek.com/print_article2/0,1217,a=139716,00.asp (Exhibit X).

deployment.[51] Workstation solutions, like those in use at Genuity at the time, would have been sufficient to meet legal requirements. The FBI's Carnivore provides a good example of a far more cost-effective solution.[52] (The SG3 Configurations provide a much more capable solution, but in my judgment the company would never have made the substantial incremental investment unless other factors were in play.)

134. Fourth, AT&T might have deployed the system in order to enhance its internal security. This is a somewhat more plausible explanation, but I believe on examination it is far from adequate to explain the investment. It is true that this configuration can be used to protect against distributed denial of service (DDoS) attacks and a number of additional security challenges, but the aggregate benefits do not approach the level of investment made.

135. I considered several alternative hypotheses, including (1) enhanced security for U.S. government customers of AT&T WorldNet; (2) data mining of AT&T customers; and (3) support for sophisticated, possibly application-specific billing and accounting measurements. None of these possibilities would appear to account for the investment that AT&T apparently made in the SG3 Configurations.

136. In sum, I can think of no business rationale in terms of AT&T's own business needs that would likely have justified an investment of this magnitude, nor any combination of rationales.

137. With that in mind, I consider it highly probable that this deployment was externally funded, and I consider the U.S. Government to be the most obvious funding source.

138. The presence of the SG3 backbone is consistent with this assessment. It is far easier to reconcile the presence of a private network with a covert project than it is to explain its presence in the context of normal AT&T operations. AT&T would most likely have used the Common Backbone for routine internal management or operational needs.

139. The SG3 Configuration is, at a technical level, an excellent fit with the requirements

---

[51] The FCC did not impose CALEA requirements on broadband or on Voice over IP (VoIP) until 2005.

[52] Marcus Thomas of the FBI described Carnivore to the North American Network Operators' Group (NANOG) in 2000. The video presentation is available at http://www.nanog.org/mtg-0010/carnivore.html; see also http://videolab.uoregon.edu/nanog/carnivore/.

of a massive, distributed surveillance project. In my opinion, and based on my experience, no other intended purpose explains as well the constellation of design choices that were made.

AT&T'S FINANCIAL CONDITION IN 2003

140. I consider it unlikely that AT&T would have made discretionary investments of this magnitude on its own initiative (with no apparent prospect of return) under any circumstances, but I consider it particularly implausible given the condition of the company in 2003.

141. Lehman Brothers issued investment guidance on AT&T on January 24, 2003, the same day on which Klein Exhibit B was issued. This guidance provides useful historic perspective on the financial state of AT&T as viewed by a knowledgeable and informed observer at the time.[53]

142. In the January 2003 assessment, Lehman Brothers lowered their target stock price from $25 to $20, and recommended that investors underweight AT&T in their portfolios. This reflects a dramatic, precipitous decline. In May 2000, their target had been $400. In January 2001, it was $200. As recently as October 2002, it had been $70.

143. The Lehman Brothers analysis shows a rapid 20% decline in revenues on the part of AT&T Consumer Services, and they predicted a 25-30% decline for 2003. 100% RBOC entry into long distance was already anticipated, as was the FCC's imminent elimination of UNE-P.[54] Lehman Brothers therefore anticipated that AT&T would be forced to exit the Consumer Services business within the year.

144. The profitability of AT&T Business Services was also under pressure – 40% of its revenues came from wholesale long distance voice, where margins were already thin and continuing to decline.

145. In short, most of the financial pressures that ultimately drove AT&T to be acquired by SBC were already evident at the time that these investments were made.

---

[53] A copy of the Lehman Brothers analysis is attached as Exhibit Y to my declaration.

[54] Regional Bell Operating Company (RBOC) entry into long distance would represent increased competition for AT&T's consumer long distance business; the FCC's phasing out of the obligation on RBOCs to provide the Unbundled Network Element Platform (UNE-P) would eliminate AT&T's ability to profitability compete with the RBOCs in offering local services. The combined effect would be to eliminate AT&T's ability to compete with the RBOCs for consumer customers seeking flat rate plans comprising both local service and long distance.

146. Given that there is no apparent revenue justification for the deployment of the SG3 Configurations, I would have expected AT&T to defer discretionary investments at that time. I therefore infer that the deployment was with high probability either externally funded or externally subsidized.

147. This assessment supports the plausibility of the Klein Declaration as regards a government role in the SG3 Configurations.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed March 29, 2006 at Bonn, Germany.

J. Scott Marcus

J. SCOTT MARCUS

DECLARATION OF SERVICE BY HAND-DELIVERY

I, the undersigned, declare:

1. That declarant is and was, at all times herein mentioned, a resident of the United States and employed in the City and County of San Francisco, over the age of 18 years, and not a party to or interested party in the within action; that declarant's business address is 100 Pine Street, Suite 2600, San Francisco, California 94111.

2. That on April 5, 2006, declarant served by Hand-Delivery the DECLARATION OF J. SCOTT MARCUS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION to the parties listed on the attached Service List.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 5th day of April, 2006, at San Francisco, California.

Marzena Poniatowska

MARZENA PONIATOWSKA

Counsel For Defendant(s)

Bruce A. Ericson

Pillsbury Winthrop Shaw Pittman LLP
50 Fremont Street
San Francisco, CA 94105-2228
415/983-1000
415/983-1200 (Fax)

Counsel For Plaintiff(s)

Cindy Cohn
Lee Tien
Kurt Opsahl
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415/436-9333
415/436-9993 (Fax)

Reed R. Kathrein
Jeff D. Friedman
Shana E. Scarlett
Lerach Coughlin Stoia Geller Rudman & Robbins LLP
100 Pine Street, Suite 2600
San Francisco, CA 94111-5238
415/288-4545
415/288-4534 (Fax)

Richard R. Wiebe
Law Office of Richard D. Wiebe
425 California Street, Suite 2025
San Francisco, CA 94104
415/433-3200
415/433-6382 (Fax)